Testimony of

Ronil Hira

Chair, R&D Policy Committee
The Institute of Electrical and Electronics Engineers - United States of America

To The

Senate Commerce, Science, and Transportation Subcommittee on Science, Technology and Space

On

Homeland Security and the Technology Sector

April 24, 2002

I would like to thank the Chairman, Ranking Member and distinguished Subcommittee Members for inviting me here today. My name is Ronil Hira, I am here on behalf of the more than 235,000 U.S. members of The Institute of Electrical and Electronics Engineers. I am the chair of IEEE-USA's Research and Development Policy Committee. Our members are electrical, electronics, computer and software engineers who work in government and industry, as private consultants and are professors and students in our universities.

We at IEEE-USA applaud the Subcommittee's efforts to address shortfalls in two critical areas related to homeland security: disaster response and mobilization, and cyber security research and development. As the nation becomes more dependent upon technology in nearly every aspect of our lives, the level of vulnerability to technological disruption rises accordingly, as does the potential impact that disruption has on our lives. As we saw with the problems that became apparent following the attacks of September 11, the promptness and quality of the technological response to terrorist attacks or natural disasters could mean the difference between life and death.

Fortunately, the United States has the largest and best-qualified pool of technological experts and the most sophisticated technology and communications equipment in the world. The challenge, however, is in coordinating the response, finding the necessary experts and supplies and getting them into place as quickly as possible.

For this reason, IEEE-USA strongly endorses the objectives of the S.2037, the Science and Technology Mobilization Act. The concept of organizing to focus the nation's technology resources to address the response to terrorist attacks and other emergencies is an important ingredient in a robust homeland defense. As a result of the attacks, local governments are renewing their efforts to design disaster-recovery plans. Many entities have put in place emergency communication plans and have taken steps to ensure optimal use of other technologies. For example, uninterruptible power supplies are now coming into common usage.

We strongly concur with Office of Science and Technology Policy Director, Dr. John Marburger's recommendation encouraging voluntary preparedness among organizations, including implementing IT disaster-recovery procedures as well as promoting standards for coordinating disaster-recovery responses. This may well fit into the charter of the National Institute of Standards and Technology; however, IEEE-USA does not take a position on which governmental agency should be charged with overseeing the overall program envisioned by the legislation. We do feel that NIST, if designated, and industry can work within the framework of a center for civilian homeland security technology evaluation as envisioned by the legislation to develop standards and protocols to serve as models for local disaster-recovery programs. The standards can not only enable optimal use of technology within a local environment, but can allow for sharing of resources to respond to a regional disaster.

The infrastructure reliability advisory board as described in the legislation can work with the center to define best practices on how to make technology and communications infrastructure less vulnerable. This will enable the board to make recommendations on all aspects of deployment of emergency response and recovery of technological and communications systems.

We urge caution in proceeding to establish the National Emergency Technology Response Teams. It is important to recognize that communication and other technological systems can be extremely complicated, requiring not only general knowledge of the technical factors but also specific knowledge of the system under stress. This may only be available in the company and its vendors that installed the system originally. Furthermore, if a local government has a sound disaster-recovery program, it may not be feasible, and could be counter-productive, to attempt to bring in teams that have not been integrated into the established program.

One valuable service that the U.S. government can perform is to evaluate and critique local disaster-recovery programs. This could consist of plan review and test observation. The Government has many agencies with expertise in this kind of service.

In regard to S.2182, the Cyber Security Research and Development Act, IEEE-USA has been a strong supporter of this legislation since the companion bill was introduced in the House of Representatives. There are many excellent provisions in this bill. I would like to highlight one in particular. The Chairman, and author of the legislation, has done a remarkable job in understanding the richness of our research enterprise and symbiotic relationships. Specifically, the bill includes research that will be conducted in universities, government and industry. Each of these institutions brings something important to the table when it comes to research.

In addition, the bill recognizes the importance of training future professionals. While some of these folks will become cyber security researchers and professors, many will become cyber security practitioners. The purpose of research is not only to advance the state of the art, but also to ultimately advance its application in the marketplace. Only through all of the mechanisms in this bill will we be able to achieve both. In order to advance the state of the art and the state of the market, we need to advance the state of the science in cyber security. Systematic research is the way in which the cyber security profession can codify its lessons learned, develop its common language, and most importantly, advance the practice of cyber security.

IEEE-USA is pleased to support S.2182, which will pay dividends not only for protection against cyber terrorism, but also for commerce and personal privacy.

Thank you very much.